日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２５日

出願番号
Application Number: 特願２０００－０１６０２０

出願人
Applicant (s): 日本電信電話株式会社

２０００年　６月２３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４６８３７

【書類名】　特許願
【整理番号】　NTTH116691
【提出日】　平成12年 1月25日
【あて先】　特許庁長官殿
【国際特許分類】　G06F
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　森田　光
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　小林　邦生
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100066153
　【弁理士】
　【氏名又は名称】　草野　卓
【選任した代理人】
　【識別番号】　100100642
　【弁理士】
　【氏名又は名称】　稲垣　稔
【手数料の表示】
　【予納台帳番号】　002897
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　大小比較装置・方法およびそのプログラム記録媒体

【特許請求の範囲】

【請求項１】　１，２，３，…，ＮのＮ種の指標値に対し、初期値ＩＶに一方向性関数ｈを多重（ここで、ＩＶにｉ回の一方向性関数を施す場合、h^i（ＩＶ）と表現し、これはｈ（ｈ（ｈ（…ｈ（ＩＶ）…））を意味し、ｈ関数をｉ回施すことを意味する。）に施した、ｈ（ＩＶ），h^2（ＩＶ），h^3（ＩＶ），…，h^N（ＩＶ）なる値をそれぞれ対応させ、

複数人の参加者Ｊ（Ｊ＝１，２，…）が、それぞれ、（$h^{N+1}(IV_J)$，ｇ（$h^i{}_J(IV_J)$））（ｇは一方向性関数を示す）なる一対の値を示すことで、意中の指標値i_Jを間接的に登録し、

指標値Ｎ，Ｎ－１，Ｎ－２，…に登録した参加者Ｊがいるかどうかを指標値の大きい順に各指標値ごとに全参加者に問合せ手段により尋ね、該当しないときは、聞かれた指標値ｍに対して各人Ｊが$h^m(IV_J)$を答えることでその回答が$h^{N+1}(IV_J)$から連なることを示し、ある参加者Ｋの指標値i_Kが聞かれた指標値ｍに該当するときになって初めて、$h^i{}_K(IV_K)$を示す事が登録されていたｇ（$h^i{}_K(IV_K)$）に対応することで、Ｎ種の指標値における最大値を予め登録していた者であることを証明する大小比較装置において、

前記１，２，３，…，ＮのＮ種の指標値に対し、P_1，P_2，P_3，…，P_Nなる値がその大小順に対応付けられている換算テーブルが設けられ、かつ参加者に公開され、P_1，P_2，P_3，…，P_Nなる値に対して登録された最大値又は最小値を求めることを特徴とする大小比較装置。

【請求項２】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nには$P_1<P_2<P_3<\cdots<P_N$なる大小関係があり、かつある特定の上位桁以上の値のみを示し、

各参加者Ｊが間接的に登録したい値が、その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、

前記一対の値（$h^{N+1}(IV_J)$，ｇ（$h^i{}_J(IV_J)$））にQ_Jを加え、（$h^{N+1}(IV_J)$，ｇ（$h^i{}_J(IV_J)$），Q_J）を登録し、

前記問合せ手段は各指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに、全参加者のQ_Jにおける大きいものから順次尋ねる手段であることを特徴とする請求項１記載の大小比較装置。

【請求項３】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nには$P_1 > P_2 > P_3 > \cdots > P_N$なる大小関係があり、かつある特定の上位桁以上の値のみを示し、

各参加者Ｊが間接的に登録したい値が、その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、

前記一対の値（$h^{N+1}(IV_J)$，$g(h^{i}_{J}(IV_J))$）にQ_Jを加え、（$h^{N+1}(IV_J)$，$g(h^{i}_{J}(IV_J))$，Q_J）を登録し、

前記問合せ手段は各指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに全参加者のQ_Jにおける小さいものから順次尋ねる手段であることを特徴とする請求項１記載の大小比較装置。

【請求項４】　１，２，３，…，ＮのＮ種の指標値に対し、初期値ＩＶに一方向性関数ｈを多重に施して、$H_1 = h(IV) \parallel f_1$，$H_2 = h(H_1) \parallel f_2$，$H_3 = h(H_2) \parallel f_3$，…，$H_N = h(H_{N-1}) \parallel f_N$なる値をそれぞれ対応させ、フラグ$f_1$～$f_N$は意中の指標値ｉの時の$f_i$とそれ以外の時のフラグとを異なる値として区別し、ｘ‖ｙはｘにｙを連結することを示し、

複数人の参加者Ｊが、それぞれ、その意中の指標値i_Jのフラグf_{iJ}を用いたｈ（H_N）なる値を示すことで、意中の指標値i_Jを間接的に登録し、

指標値Ｎ，Ｎ－１，Ｎ－２，…に登録した参加者Ｊがいるかどうかを指標値の大きい順に各指標値ごとに全参加者に問合せ手段により尋ね、該当しないときは、聞かれた指標値ｍに対して$H_m = h(H_{m-1}) \parallel f_m$に相当する値を各人が答えることでその回答がｈ（$H_N$）から連なることを示すとともに$f_m$により意中の値でないことを示し、ある参加者Ｋの指標値i_Kが聞かれた指標値ｍに該当するときになって初めて、$H_{iK} = h(H_{iK-1}) \parallel f_{iK}$を示し$f_{iK}$が意中の値にあることを示すことで、Ｎ種の指標値における最大値を予め登録していた者であることを証明する大小比較装置において、

前記、１，２，３，…，ＮのＮ種の指標値に対し、P_1，P_2，P_3，…，Ｐ

$_N$ なる値がその大小順に対応付けられている換算テーブルが設けられ、かつ参加者に公開され、P_1，P_2，P_3，…，P_Nなる値に対して登録された最大値又は最小値を求めることを特徴とする大小比較装置。

【請求項５】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nなる値には$P_1<P_2<P_3<\cdots<P_N$なる大小関係があり、かつ上位桁以上の値のみを示し、

各参加者Ｊが間接的に登録したい値が、その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、

前記$H_{(N+1)J}=h(H_{NJ})$にQ_Jを加え、$(H_{(N+1)J}, Q_J)$を登録し、

前記問合せ手段は、指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに全参加者のQ_Jにおける大きいものから順次尋ねる手段であることを特徴とする請求項４記載の大小比較装置。

【請求項６】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nなる値には$P_1>P_2>P_3>\cdots>P_N$なる大小関係があり、かつ上位桁以上の値のみを示し、

各参加者Ｊが間接的に登録したい値が、その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、

前記$H_{(N+1)J}=h(H_{NJ})$にQ_Jを加え、$(H_{(N+1)J}, Q_J)$を登録し、

前記問合せ手段は指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに全参加者のQ_Jにおける小さいものから順次尋ねる手段であることを特徴とする請求項４記載の大小比較装置。

【請求項７】　１，２，３，…，ＮのＮ種の指標値に対応して、初期値ＩＶに一方向性関数ｈを多重（ここで、ＩＶにｉ回の一方向性関数を施す場合、h^i（ＩＶ）と表現し、これはｈ（ｈ（ｈ（…ｈ（ＩＶ）…））を意味し、ｈ関数をｉ回施すことを意味する）に施した、ｈ（ＩＶ），h^2（ＩＶ），h^3（ＩＶ），…，h^N（ＩＶ）なる値をそれぞれ対応させることとし、

各参加者Ｊは、前記１，２，…，Ｎの指標値に対し、P_1，P_2，…，P_Nなる値がその大小順に対応付けられている換算テーブルを参照して登録したい値と対応する指標値i_Jを求めて参加者端末装置により（$h^{N+1}(IV_J)$，$g(h^i{}_J, (IV_J))$）なる一対の値を作成して中央装置へ送って意中の指標値i_Jを間接的に登録し、

中央装置は全ての参加者からの登録値を受信した後、

指標値Ｎ，Ｎ－１，Ｎ－２，…に登録した参加者Ｊがいるかどうかを、指標値の大きい順に各指標値ごとに全参加者端末装置に該当指標値ｍの問合せ情報を送って尋ね、

参加者端末装置は受信した問合せ情報に対し該当しないときは、聞かれた指標値ｍに対してh^{m}（IV_J）を生成して前記中央装置へ送信し、

前記中央装置は受信したh^{m}（IV_J）がh^{N+1}（IV_J）から連なることを確認し、

前記問合せに対し参加者Ｋの指標値i_Kが該当するときはその参加者端末装置は少くともh^{i}_{K}（IV_K）を生成して前記中央装置へ送信し、

前記中央装置は受信したh^{i}_{K}（IV_K）からｇ（h^{i}_{K}（IV_K））を生成し、これが先に登録したものと対応することを確認して、その指標値i_Kにて前記換算テーブルを参照して値P_{iK}を求め、その参加者Ｋが登録値P_{iK}が登録中の最大値又は最小値であることを出力することを特徴とする大小比較方法。

【請求項８】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nには$P_1<P_2<P_3<\cdots<P_N$なる大小関係があり、かつ上位桁以上の値のみを示し、

参加者Ｊが間接的に登録したい値が、

その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、前記参加者端末装置で（h^{N+1}（IV_J），ｇ（h^{i}_{J}（IV_J））にＱ$_J$を加え、（h^{N+1}（IV_J），ｇ（h^{i}_{J}（IV_J）），Q_J）を前記中央装置へ送って登録し、

前記中央装置は各指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに、全参加者のQ_Jにおける大きいものから順次前記問合せを行うことを特徴とする請求項７記載の大小比較方法。

【請求項９】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nが$P_1>P_2>P_3>\cdots>P_N$なる大小関係があり、かつ、上位桁以上の値のみを示し、

参加者Ｊが間接的に登録したい値が、その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、前記参加者端末装置は（h^{N+1}（IV_J），ｇ（h^{i}_{J}（IV_J）），Q_J）を前記中央装置へ送

って登録し、

前記中央装置は各指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに全参加者のQ_Jにおける小さいものから順次前記問合せを行うことを特徴とする請求項７記載の大小比較方法。

【請求項１０】　１，２，３；…，ＮのＮ種の指標値に対応して、初期値ＩＶに一方向性関数ｈを多重に施して、$H_1=h(IV)\|f_1$，$H_2=h(H_1)\|f_2$，$H_3=h(H_2)\|f_3$，…，$H_N=h(H_{N-1})\|f_N$なる対応値をそれぞれ対応させ、フラグf_1～f_Nは意中の指標値ｉの時のf_iとそれ以外の時のフラグとを異なる値として区別し、ｘ‖ｙはｘにｙを連結することを示し、

各参加者Ｊは前記１，２，…，Ｎの指標値に対し、P_1，P_2，…，P_Nなる値がその大小順に対応付けられている換算テーブルを参照して登録したい値と対応する指標値i_Jのフラグf_{iJ}を用いて参加者端末装置により$h(H_N)$なる値を生成して中央装置へ送って意中の指標値i_Jを間接的に登録し、

前記中央装置は全ての参加者からの登録値を受信した後、

指標値Ｎ，Ｎ－１，Ｎ－２，…に登録した参加者Ｊがいるかどうかを、指標値の大きい順に各指標値ごとに全参加者端末装置に該当指標値ｍの問合せ情報を送って尋ね、

参加者端末装置は受信した問合せ情報に対し該当しないときは、聞かれた指標値ｍに対して$H_m=h(H_{m-1})\|f_m$に相当する値を生成して前記中央装置へ送信し、

前記中央装置は受信した$H_m=h(H_{m-1})\|f_m$が$h(H_N)$から連なることを確認し、

かつf_mにより意中の値でないことを確認し、

前記問合せに対し参加者Ｋの指標値i_Kが該当するときはその参加者端末装置は、$H_{iK}=h(H_{iK-1})\|f_{iK}$を前記中央装置へ送信し、

前記中央装置はその受信した$H_{iK}=h(H_{iK-1})\|f_{iK}$と共に登録したものとから登録したものであることを確認し、その指標値i_Kにて前記換算テーブルを参照して値P_{iK}を求め、その参加者Ｋが登録値P_{iK}が登録中の最大値又は最小値であることを特徴とする大小比較方法。

【請求項１１】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nが$P_1<P_2<P_3<\cdots<P_N$なる大小関係があり、かつ上位桁以上の値のみを示し、

参加者Ｊが間接的に登録したい値が、その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、前記参加者端末装置は（h（H_{NJ}），Q_J）を、前記中央装置へ送って登録し、

前記中央装置は各指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに、全参加者のQ_Jにおける大きいものから順次前記問合せを行うことを特徴とする請求項１０記載の大小比較方法。

【請求項１２】　前記変換テーブルは前記P_1，P_2，P_3，…，P_Nが$P_1>P_2>P_3>\cdots>P_N$なる大小関係があり、かつ上位桁以上の値のみを示し、

参加者Ｊが間接的に登録したい値が、その上位桁の値と該当する指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jとの和$P_{iJ}+Q_J$で表現されるとき、前記参加者端末装置は（h（H_{NJ}），Q_J）を前記中央装置へ送信して登録し、

前記中央装置は指標値Ｎ，Ｎ－１，Ｎ－２，…ごとに全参加者のQ_Jにおける小さいものから順次前記問合せを行うことを特徴とする請求項１０記載の大小比較方法。

【請求項１３】　中央装置に登録値を登録し、中央装置で複数の参加者からの登録値中の最大値又は最小値を決めてもらう参加者端末装置のコンピュータに、

上位桁の指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jよりなる登録値を入力する処理と、

参加者の固有の初期値IV_Jに対してＮ＋１回多重一方向性関数ｈを施した値$h^{N+1}(IV_J)$（Ｎは指標値の種類の数）を生成する処理と、

IV_Jに対しｉＪ回多重一方向性関数ｈを施し、更に一方向性関数ｇを施した値ｇ（$h^{i}_{J}(IV_J)$）を生成する処理と、

上記$h^{N+1}(IV_J)$と上記ｇ（$h^{i}_{J}(IV_J)$）と上記Q_Jを登録情報A_Jとして中央装置へ送信する処理と、

中央装置からの指標値ｋを登録したかの問合せを受信する処理と、

上記受信したｋについて$h^{k}(IV_1)$を生成する処理と、

上記h^k（IV_1）を上記中央装置に送信する処理と
を実行させるプログラムを記録した記録媒体。

【請求項１４】　中央装置に登録値を登録し、中央装置で複数の参加者からの登録値中の最大値又は最小値を決めてもらう参加者端末装置のコンピュータに、

上位桁の指標値i_Jと対応する値P_{iJ}と下位桁の値Q_Jよりなる登録値を入力する処理と、

参加者の固有の初期値IV_Jに対し一方向性関数hを多重に施して$H_1=h(IV_J)\|f_1$，$H_2=h(H_1)\|f_2$，$H_3=h(H_2)\|f_3$，…，$H_N=h(H_{N-1})\|f_N$，$h(H_N)$（Nは指標値の種類の数、f_1～f_Nはフラグでその１つはf_{iJ}であり、これは他のフラグと異なる値）を生成する処理と、

上記$h(H_N)$とQ_Jを登録情報A_Jとして中央装置へ送信する処理と、

中央装置から指標値mを登録したかの問合せを受信する処理と、

上記受信mに対し、$H_m=h(H_{m-1})\|f_m$を生成する処理と、

上記$H_m=h(H_{m-1})\|f_m$を上記中央装置に送信する処理と
を実行させるプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、例えば電子競争入札方法に適用され、複数人の意中の値を比較する際に、最大または最小の意中の値を持つ者の値は知らせるが、それ以外の者の値は秘密裏にできる大小比較装置・方法およびそのプログラム記録媒体に関するものである。

【０００２】

【従来の技術】

例えば電子競争入札は図９に示す様に、参加者毎に設けられる入札装置11_1，11_2，…，11_Mと、これらと例えばネットワークで接続され、全体を統合的に処理する開票装置１２から構成され、各１，２，３，…，NのN種の指標値に対応して、初期値IVに一方向性関数hを多重に施し、つまりIVにi回の一方

向性関数を施す場合、h^i（ＩＶ）と表現し、これはｈ（ｈ（ｈ（…ｈ（ＩＶ）…））））とｈをｉ回施すことを意味する。これらｈ（ＩＶ），h^2（ＩＶ），h^3（ＩＶ），…，h^N（ＩＶ）なる値をそれぞれ指標値１，２，３，…，Ｎと対応させることとし、各参加者Ｊ（Ｊ＝１，２，…，Ｍ）はその入札装置11_JからA_J＝（h^{N+1}（IV_J），ｇ（$h^i{}_J$（IV_J））なる一対の値を生成して、開票装置１２に送ることで、その参加者Ｊの意中の指標値i_Jを間接的に登録する。ｇ（ｘ）はｘに一方向性関数ｇを施すことを表わす。開票装置１２は全参加者からの登録を受信した後、カウンタ１３を初期値Ｎから順次ダウンカウントし、そのカウンタ１３の各値ｋ（Ｎ，Ｎ－１，…，１）について登録した参加者Ｊがいるかどうかを、全参加者端末装置11_1，…，11_Mに順次ｋを送信して尋ね、毎回、該当しないときは、聞かれた指標値ｋに対してh^k（IV_J）に相当する値B_Jを各参加者装置11_Jから開票装置１２へ応答することでh^{N+1}（IV_J）から連なることを示し、ある参加者Ｋの指標値i_Kが該当するときになって初めて、$h^i{}_K$（IV_K）が開票装置１２に受信され、これがその登録されていたｇ（$h^i{}_K$（IV_K））に対応することで、登録された指標値中の最大値を予め登録していた者であることを証明する。このようにして開票装置は登録指標の大小比較を行うことが提案されている（例えば、特願平１１－２０５００４号）。

【０００３】

この装置では前記１，２，３，…，ＮのＮ種の指標値にそれぞれ対応しているP_1，P_2，P_3，…，P_Nなる値が$P_1<P_2<P_3<\cdots<P_N$なる大小関係が成立している場合には対応できるが、$P_1>P_2>P_3>\cdots>P_N$なる大小関係が成立している場合にはそのままでは対応できなかった。

また、第２の問題として、比較対象のＮ種の指標値が限定される場合、例えば、１～１億までの数を区別したくても、Ｎが限定され、例えば、一万種しか無かった場合、便宜的に１万刻みに、１万，２万，…，９９９９万，１億という表現しかゆるされなかった。しかし、本当は１刻みで大小判定をしたかったが、このようなことは従来は実質的にはできなかった。

【０００４】

【発明が解決しようとする課題】

この発明の目的は一種の大小判定の機能により、最大値検出と最小値検出の両方を同一の手法で実行できる大小比較方法を提供することにある。

この発明の他の場合は指標値の表現種類が限定される場合でも、任意の桁の範囲で大小判定をすることを可能にする比較方法を提供することにある。

【０００５】

【課題を解決するための手段】

第一の課題は、内部的な指標値と外部的な対応値の対応付けを与える手段を設けることにより、同じ演算機能を最大または最小の複数の目的で使えることにする。

第二の課題は、前記外部的な対応値において、ある桁以上は大小判定にとって重要なので秘密裏に扱うが、その桁未満は公開しても、実質的な重要性が低いので、下の桁の大小により比較の順番をつけて公表する手段を設け、任意の桁の範囲での大小比較を可能とする。

【０００６】

【発明の実施の形態】

以下図面を用いてこの発明の実施例について詳しく説明する。

第一の実施例

電子競争入札を例とした場合で、図１に示すように複数の参加者Ｊ（Ｊ＝１，２，…，Ｍ）の入札装置１１$_J$と開票装置１２とで構成され、これらは通信手段で互いに接続することが可能である。入札装置１１$_J$は１つしか示していないが複数存在する。この実施例では内部的な指標値１，２，…，Ｎと外部的な対応値１０，１５，…，３０００との対応付けを示す換算テーブル２１が入札装置１１$_J$、開票装置１２にそれぞれ設けられている。

【０００７】

１，２，３，…，ＮのＮ種の指標値ｋに対応して、初期値ＩＶに一方向性関数ｈを多重（例えば、ＩＶにｉ回の一方向性関数を施す場合、h^i（ＩＶ）と表現することにする。但し、意味はｈとｉ回施すｈ（ｈ（ｈ（…ｈ（ＩＶ）…））と同様である）に施した、ｈ（ＩＶ），h^2（ＩＶ），h^3（ＩＶ），…，h^N（ＩＶ）なる値をそれぞれ対応させることとし、各参加者Ｊは意中の指標値ｋがｉ

$_J$の場合入札装置１１$_J$により（h^{N+1}（ＩＶ$_J$），ｇ（$h^i{}_J$（ＩＶ$_J$））なる一対の値を生成し、これら開票装置１２へ送信することにより意中の指標値ｉ$_J$を間接的に登録する。

【０００８】

全参加者からの登録が終了した後、開票装置１２はカウンタ１３に最大指標値Ｎを初期値として設定し、このカウンタ１３の値ｋ＝Ｎを登録した参加者Ｊがいるかどうかを全参加者の入札装置１１$_J$にｋ＝Ｎを送って尋ねる。入札装置１１$_J$はその問合せに該当しないときは、聞かれた指標値ｋに対してh^k（ＩＶ$_J$）を生成して開票装置１２へ送って回答する。開票装置１２はその受信したh^k（ＩＶ$_J$）が先に登録したh^{N+1}（ＩＶ$_J$）から連なることを知る。全参加者から回答が該当しない時はカウンタ１３を１ダウンカウントしてｋ＝Ｎ－１として同様の問合せを行う。以下同様のことを行う。ある参加者の指標値ｉ$_K$が該当するときになって初めてその入札装置１１$_K$から受信した$h^i{}_K$（ＩＶ$_K$）に対しｇ（$h^i{}_K$（ＩＶ$_K$）を求め、これが登録されていたｇ（$h^i{}_K$（ＩＶ$_K$））と一致することで、指標における最大値を予め登録していた者であることを証明する。

【０００９】

この場合は換算テーブル２１において１，２，３，…，ＮのＮ種の指標値に対応した外部的対応値Ｐ$_1$，Ｐ$_2$，Ｐ$_3$，…，Ｐ$_N$なる値はＰ$_1$＜Ｐ$_2$＜Ｐ$_3$＜…＜Ｐ$_N$なる大小関係が成立するように対応付けられてある。従って前述したように開票装置１２で登録されている指標値中の最大値が検出されるから、その最大値の登録指標値ｉ$_k$と対応する外部的対応値Ｐ$_{ik}$は各参加者が意中の登録した値中の最大値を示すことになる。

【００１０】

なお開票装置１２は全参加者が登録後にその登録値（h^{N+1}（ＩＶ$_J$），ｇ（$h^i{}_J$（ＩＶ$_J$））を出力公開し、また求めた最大登録指標値ｉ$_J$と、その登録参加者Ｊを出力表示する。

第二の実施例

この実施例は図２に示す様に、図１に示した構成とほぼ同様であり、その指標値の開票装置１２への登録、開票装置１２における登録最大指標値とその参加者

を求める処理も同様である。

【００１１】

第一の実施例と異なる点は、換算テーブル２１の内容である。つまりこの場合の換算テーブル２１において１，２，３，…，ＮのＮ種の指標値に対応した外部的対応値P_1，P_2，P_3，…，P_Nなる値は$P_1>P_2>P_3>\cdots>P_N$なる大小関係が成立するように対応付けられてある。図２の例では指標値１は３０００、２は２９１３、３は２９００と指標値が大きくなるに従って外部的対応値P_kは小さくなる。従って求められた登録指標値中の最大値i_Kと対応する外部的対応値P_{i_k}は全参加者が意中の登録した値中の最小値を示すことになる。

【００１２】

このようにこの発明では換算テーブル２１の指標値と対応値との大小関係を逆にすることにより、同一構成、同一処理手順で最大値を求めることも最小値を求めることの何れにも変更できる。

第三の実施例

第三の実施例は図３に示す様に、入札装置11_J、開票装置１２、共通の換算テーブル２１を備えることは第一の実施例と同一である。

【００１３】

ただ処理が以下のように異なる。１，２，３，…，ＮのＮ種の指標値に対応して、初期値ＩＶに一方向性関数ｈを多重に施して、$H_1=h(IV)\parallel f_1$，$H_2=h(H_1)\parallel f_2$，$H_3=h(H_2)\parallel f_3$，…，$H_N=h(H_{N-1})\parallel f_N$なる値をそれぞれ対応させる。フラグ$f_1$～$f_N$は意中の指標値ｉの時の$f_i$とそれ以外の時のフラグと異なる値として区別できるものとする。例えば入札指標値のフラグf_iは１とし、非入札指標値ｐのフラグf_pは０とする。ｘ‖ｙはｘにｙを連結することを示すとき、参加者Ｊは入札装置11_Jで初期値IV_Jに対し、前記多重に一方向性関数ｈを施すがその際、連結するフラグｆを、入札したい指標値に対しては例えば１とし、その他の指標値と対応するフラグは０としてｈ（H_N）を生成して意中の指標値i_Jを間接的に登録する。

【００１４】

全参加者の登録が終った後、開票装置１２は指標値Ｎ，Ｎ－１，Ｎ－２，…の

それぞれごとに登録した参加者Ｊがいるかどうかを登録指標値を全参加者の入札装置に送って尋ね、入札装置は該当しないときは、聞かれた指標値ｋに対して$H_k = h(H_{k-1}) \| f_k$に相当する値を開票装置１２へ返送することでｈ（H_N）から連なることを示すとともにf_kにより意中の値でないことを示し、ある参加者Ｋの指標値i_Kが該当するときになって初めて、その入札装置11_Kから送られた$H_{iK} = h(H_{iK-1}) \| f_{iK}$が登録してあるものと一致し、その$f_{iK}$が意中の指標値にあることが求まる。この指標値が登録中の最大値であり、その回答がその指標値を予め登録していた者であることを証明することができる。なお、この明細書においては例えば$i_K - 1$を添字として用いる時はｉＫ－１と表し、他の添字も同様である。

【００１５】

この場合換算テーブル２１の１，２，３，…，ＮのＮ種の指標値に対応する、P_1，P_2，P_3，…，P_Nなる値は$P_1 < P_2 < P_3 < \cdots < P_N$なる大小関係が成立するようにされてある。よって求めた登録最大値の指標値i_Kは最大入札値P_{iK}となる。

第四の実施例

図４に示す様に、図３に示した場合と同様の構成、同様の処理を行うが、換算テーブル２１は１，２，３，…，ＮのＮ種の指標値に対応する、P_1，P_2，P_3，…，P_Nなる値が$P_1 > P_2 > P_3 > \cdots > P_N$なる大小関係が成立しているようにされてある。従って、求めた登録最大値の指標値i_Kは最小入札値P_{iK}となる。

第五の実施例

図５に示す様に、図１に示した構成と同様であり、処理もほぼ同様であるが、換算テーブル２１において指標値１，２，３，…，Ｎと対応する値P_1，P_2，P_3，…，P_Nは$P_1 < P_2 < P_3 < \cdots < P_N$なる大小関係が成立していることも同様であるが、これらP_1，P_2，P_3，…，P_Nはある桁以上の値、つまり上位桁の値のみを示し、図では指標値１は１０００、２は２０００、３は３０００…と４桁以上の値である。

【００１６】

参加者Ｊが入札したい値を、その上位桁（前記ある桁）以上の値と該当する指

標値i_Jと対応する値P_{iJ}と下位桁の値、つまり前記ある桁未満の値Q_Jとの和$P_{iJ}+Q_J$で表現し、図１で生成した（$h^{N+1}(IV_J)$，$g(h^i{}_J(IV_J))$）にQ_Jを加え、（$h^{N+1}(IV_J)$，$g(h^i{}_J(IV_J))$，Q_J）を開票装置１２へ送って登録する。

開票装置１２は各指標値についてその大きい順に参加者の入札装置に問合せを行うが、各指標値ごとに、全参加者のQ_Jにおける大きいものから（降順に）順次尋ねる。聞いた指標値に対し、登録した参加者が求まれば、その問合せ指標値についてまだ問合せをしていない参加者がいても、以後の問合せを中止する。なお問合せｋに対し、$h^k(IV_J)$を回答することは図１の場合と同様である。

【００１７】

以上のようにして指標値の種類が少なく、複数人が例え同じ対応値P_iまたは指標値ｉを指定したとしても、ある桁以下のQ_J値の大小により互いに区別し、真に最大値となる参加者および値を示すことができる。

第六の実施例

図６に示す様に、図５と同様な構成であるが、換算テーブル２１において指標値１，２，３，…，Ｎと対応する値P_1，P_2，P_3，…，P_Nが$P_1>P_2>P_3>\cdots>P_N$なる大小関係とされてあり、かつある桁以上の値のみを示す価である。参加者Ｊが間接的に登録したい値を、ある桁以上の値の指標値i_Jと対応する値P_{iJ}と前記桁未満の値Q_Jとの和$P_{iJ}+Q_J$で表現し、図５の場合と同様に（$h^{N+1}(IV_J)$，$g(h^i{}_J(IV_J))$，Q_J）を開票装置１２へ送り登録する。

【００１８】

開票装置１２は各指標値ごとの登録をしているかの問合せを大きい順、つまりＮからＮ－１，Ｎ－２，…と行うが、その各指標値ごとに全参加者のQ_Jにおける小さいものから（昇順に）順次尋ね、参加者の回答が登録したものとなる場合にその指標値についての問合せが済んでなくても問合せを中止する。

以上のようにして指標値の種類が少なく、複数人が例え同じ対応値P_iまたは指標値ｉを指定したとしても、ある桁以下のQ_J値の大小により互いに区別し、真に最小値となる参加者および値を示すことができる。

第七の実施例

図７に示す様に、図３に示した構成及び処理とほぼ同様であるが換算テーブル２１は図５に示したものと同様なものが用いられ、従って参加者Ｊが間接的に登録したい値を、図５で説明したように$P_{iJ}+Q_J$と表現し、入札装置から$H_{(N+1)J}=h(H_{NJ})$にQ_Jを加え、$(H_{(N+1)J}, Q_J)$を開票装置１２へ送信して登録する。

【００１９】

開票装置１２での各指標値についての登録したかの問合せは図５の実施例と同様に指標値Ｎから、Ｎ－１，Ｎ－２，…に対応するP_{iJ}を登録した参加者Ｊがいるかどうかを、各指標値ごとに全参加者のQ_Jにおける大きいものから（降順に）順次尋ねる。

問合せｍに対し$H_m=h(H_{m-1})\parallel f_m$を応答することは図３の場合と同様である。

【００２０】

このようにして指標値の種類が少なく、複数人が例え同じ対応値P_iまたは指標値ｉを指定したとしても、ある桁以下のＱ値の大小により互いに区別し、真に最大値となる参加者および値を示すことができる。

第八の実施例

図８に示す様に、図４に示した構成及び処理とほぼ同様であるが換算テーブル２１は図６に示したものが用いられ、入札値の登録は図７の場合と同様に参加者Ｊが間接的に登録したい値を$P_{iJ}+Q_J$で表現し、$H_{(N+1)J}=h(H_{NJ})$にQ_Jを加え、$(H_{(N+1)J}, Q_J)$を送信登録する。

【００２１】

開票装置１２で各指標値ごとにその大きい順から対応するP_{iJ}を登録した参加者Ｊがいるかどうかを、全参加者のQ_Jにおける小さいものから（昇順に）順次尋ねる。

このようにして指標値の種類が少なく、複数人Ｊが例え同じ対応値P_{iJ}または指標値i_Jを指定したとしても、ある桁以下のQ_J値の大小により互いに区別し、真に最小値となる参加者および値を示すことができる。上述ではこの発明を電子競争入札方法に適用したが、その他の場合でも複数の参加者が中央装置にある値

を登録し、その最大値又は最小値を求め、それ以外のものを明かさずに済む場合に適用できる。また上述の各装置はコンピュータによりプログラムを解読実行させて機能させることもできる。

【００２２】

【発明の効果】

上記各種実施例に示す様に、第一～第四の実施例によれば、Ｎ種類の値に関して大小比較する装置により、最大値選定または最小値選定を、選定されないものの価を明かさずに実行できる。また、第五～第八の実施例によれば、値がＮ種以上の表現範囲がある比較において、中央装置によって比較する部分を上位桁に限定し、下位の桁は予め明かし、大小比較時においても順番付けをすることにより、Ｎ種類の値に関して大小比較する装置により、最大値選定または最小値選定を選定されないものの価を明かさずに実行できる。

【図面の簡単な説明】

【図１】

第一の実施例を示す図。

【図２】

第二の実施例を示す図。

【図３】

第三の実施例を示す図。

【図４】

第四の実施例を示す図。

【図５】

第五の実施例を示す図。

【図６】

第六の実施例を示す図。

【図７】

第七の実施例を示す図。

【図８】

第八の実施例を示す図。

【図９】

提案されている電子競争入札装置を示す図。

【書類名】　　図面

【図１】

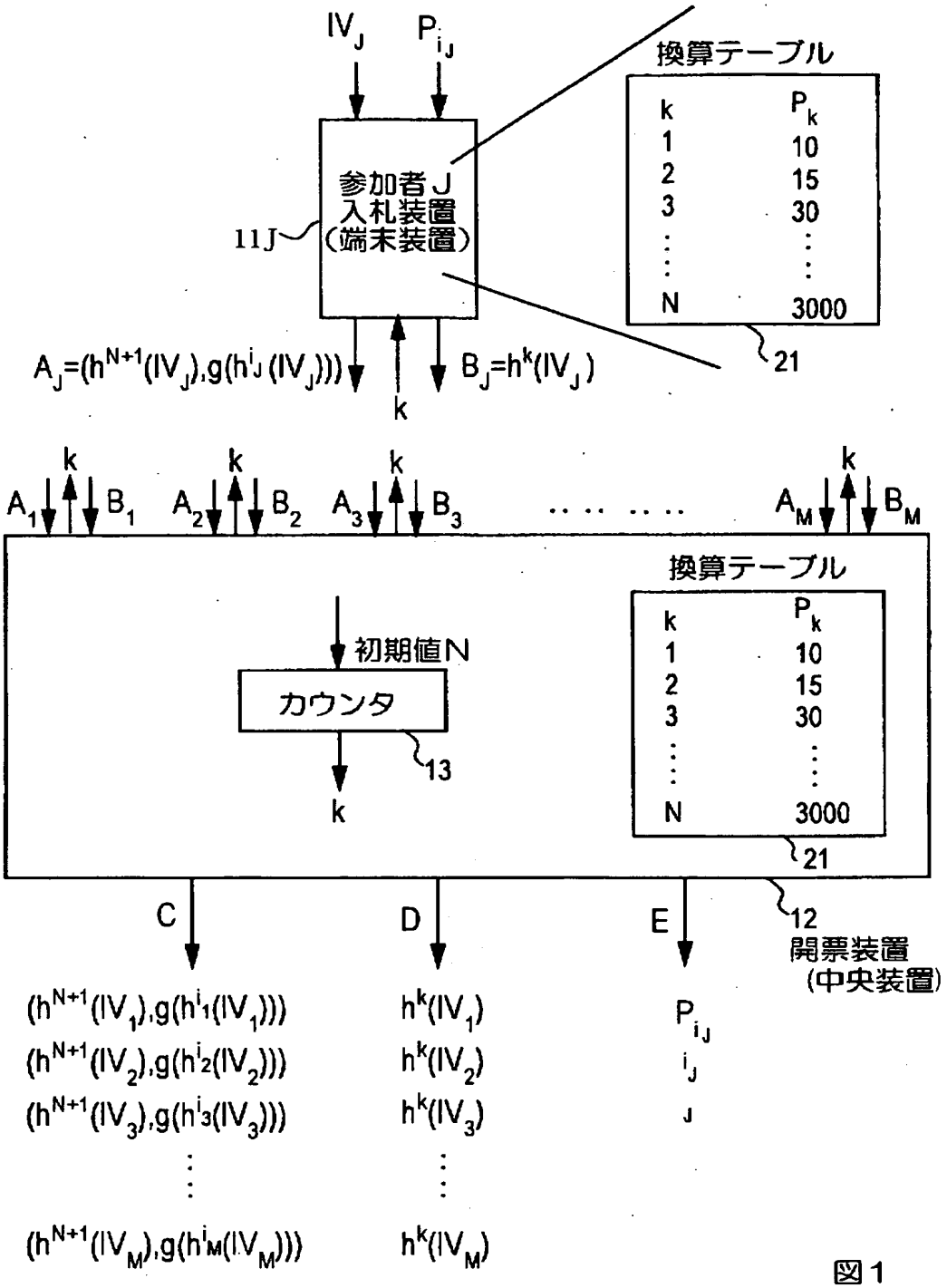

図１

出証特２０００－３０４６８３７

【図２】

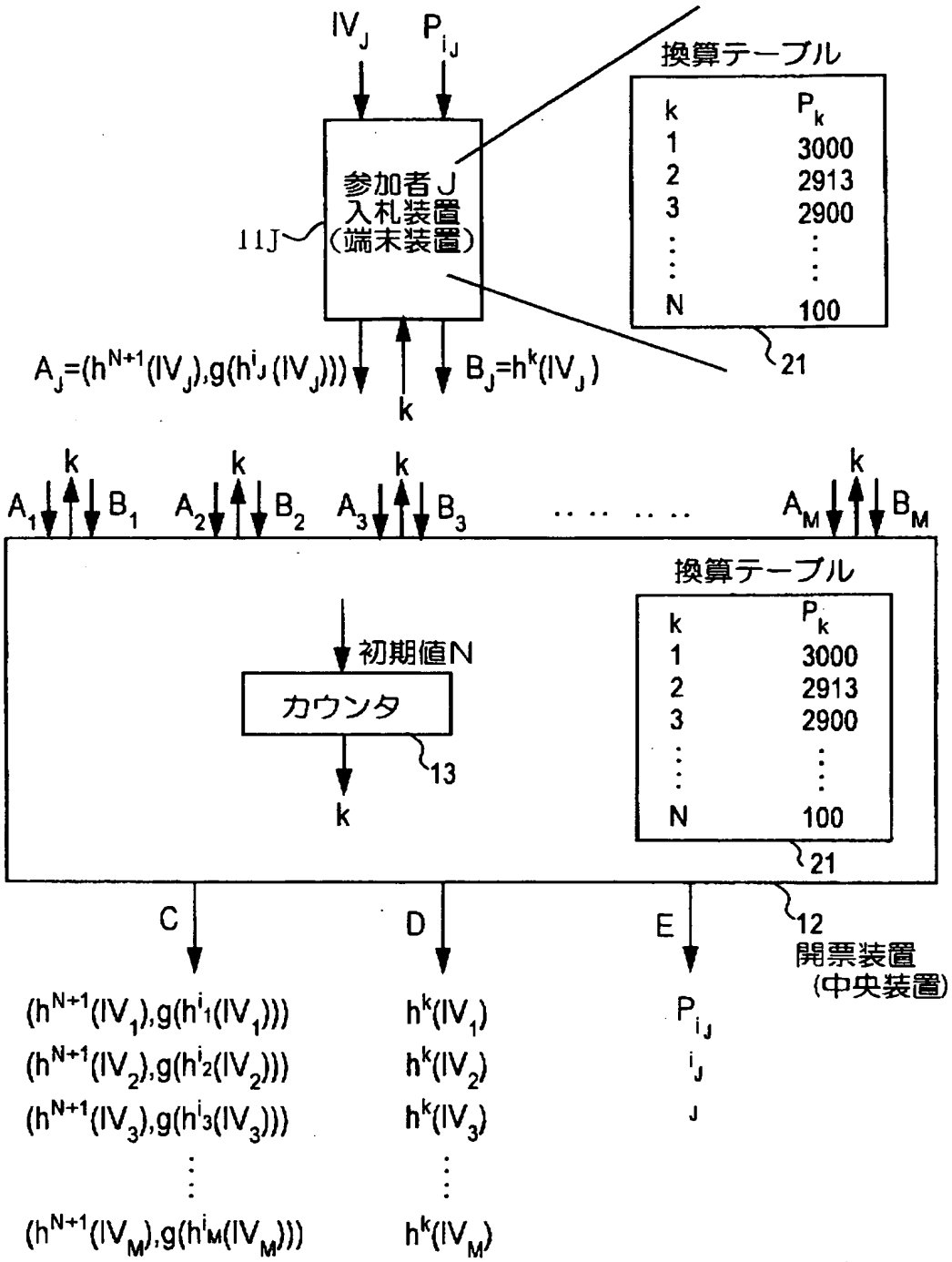
IV_J
P_iJ
換算テーブル
k
P_k
1
3000
2
2913
3
2900
N
100
参加者Ｊ
入札装置
(端末装置)
11J
21
A_J=(h^N+1(IV_J),g(h^iJ(IV_J)))
B_J=h^k(IV_J)
k
A_1
B_1
A_2
B_2
A_3
B_3
A_M
B_M
初期値N
カウンタ
13
12
開票装置
(中央装置)
C
D
E
(h^N+1(IV_1),g(h^i1(IV_1)))
(h^N+1(IV_2),g(h^i2(IV_2)))
(h^N+1(IV_3),g(h^i3(IV_3)))
(h^N+1(IV_M),g(h^iM(IV_M)))
h^k(IV_1)
h^k(IV_2)
h^k(IV_3)
h^k(IV_M)
P_iJ
iJ
J

図2

【図３】

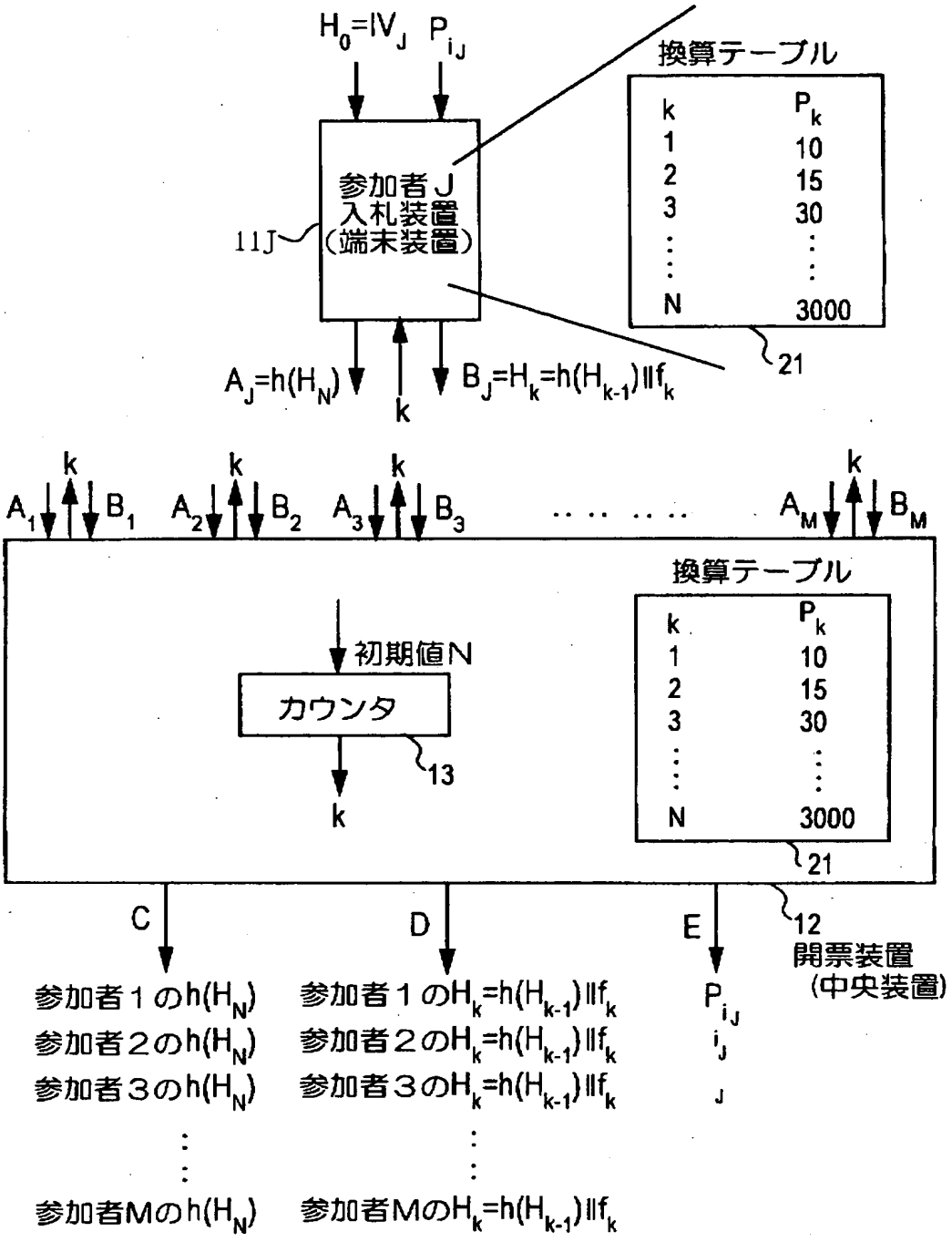
$H_0=IV_J$ P_{iJ}
換算テーブル
k P_k
1 10
2 15
3 30
N 3000
参加者Ｊ
入札装置
(端末装置)
11J
21
$A_J=h(H_N)$
k
$B_J=H_k=h(H_{k-1})\|f_k$
A_1 B_1 A_2 B_2 A_3 B_3 A_M B_M
初期値N
カウンタ
13
C
D
E
12
開票装置
(中央装置)
参加者１の$h(H_N)$
参加者２の$h(H_N)$
参加者３の$h(H_N)$
参加者Mの$h(H_N)$
参加者１の$H_k=h(H_{k-1})\|f_k$
参加者２の$H_k=h(H_{k-1})\|f_k$
参加者３の$H_k=h(H_{k-1})\|f_k$
参加者Mの$H_k=h(H_{k-1})\|f_k$
P_{iJ}
i_J
J

図3

【図４】

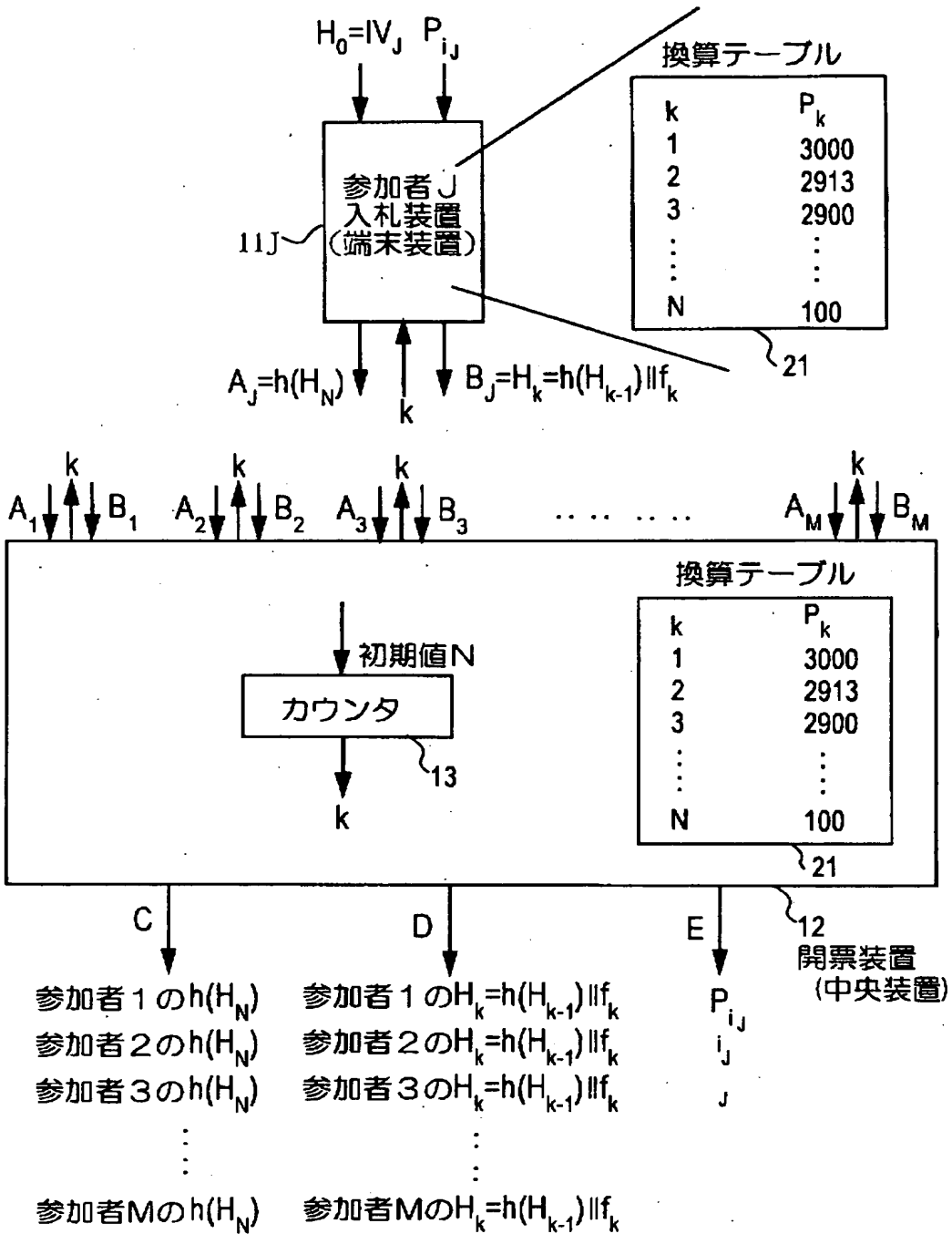
$H_0=IV_J$ P_{iJ}
参加者Ｊ
入札装置
(端末装置)
11J
換算テーブル
k P_k
1 3000
2 2913
3 2900
N 100
21
$A_J=h(H_N)$
k
$B_J=H_k=h(H_{k-1})\|f_k$
A_1 B_1 A_2 B_2 A_3 B_3 A_M B_M
初期値N
カウンタ
13
12
開票装置
(中央装置)
C
D
E
参加者１の$h(H_N)$
参加者２の$h(H_N)$
参加者３の$h(H_N)$
参加者Mの$h(H_N)$
参加者１の$H_k=h(H_{k-1})\|f_k$
参加者２の$H_k=h(H_{k-1})\|f_k$
参加者３の$H_k=h(H_{k-1})\|f_k$
参加者Mの$H_k=h(H_{k-1})\|f_k$
P_{iJ}

図４

【図５】

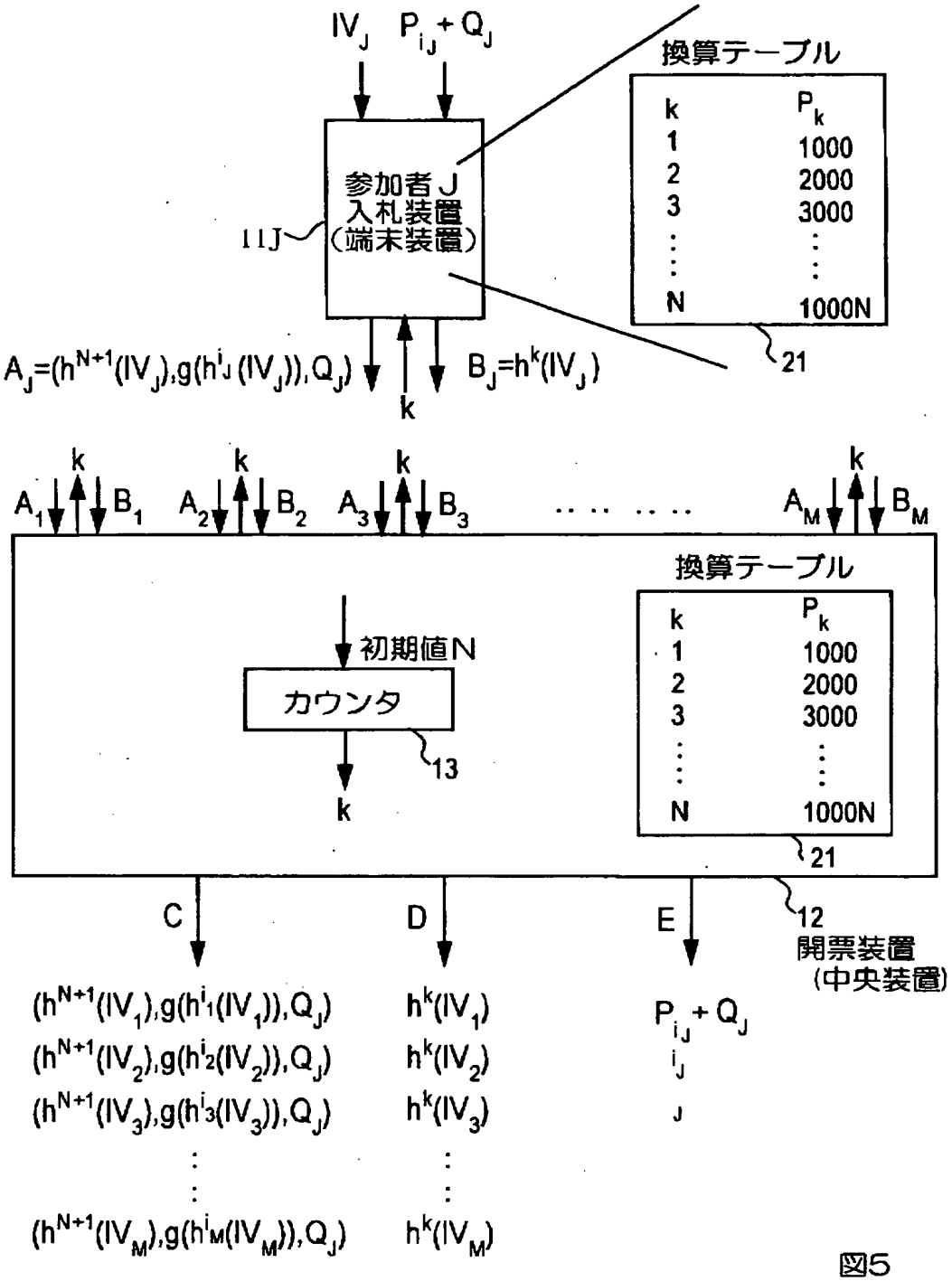
IV_J
P_iJ + Q_J
換算テーブル
k
P_k
1
1000
2
2000
3
3000
N
1000N
21
参加者Ｊ
入札装置
（端末装置）
11J
A_J=(h^N+1(IV_J),g(h^iJ(IV_J)),Q_J)
B_J=h^k(IV_J)
k
A_1 B_1 A_2 B_2 A_3 B_3 ... A_M B_M
初期値N
カウンタ
13
12
開票装置
（中央装置）
C
D
E
(h^N+1(IV_1),g(h^i1(IV_1)),Q_J)
h^k(IV_1)
(h^N+1(IV_2),g(h^i2(IV_2)),Q_J)
h^k(IV_2)
(h^N+1(IV_3),g(h^i3(IV_3)),Q_J)
h^k(IV_3)
(h^N+1(IV_M),g(h^iM(IV_M)),Q_J)
h^k(IV_M)
P_iJ + Q_J
i_J
J

図5

【図６】

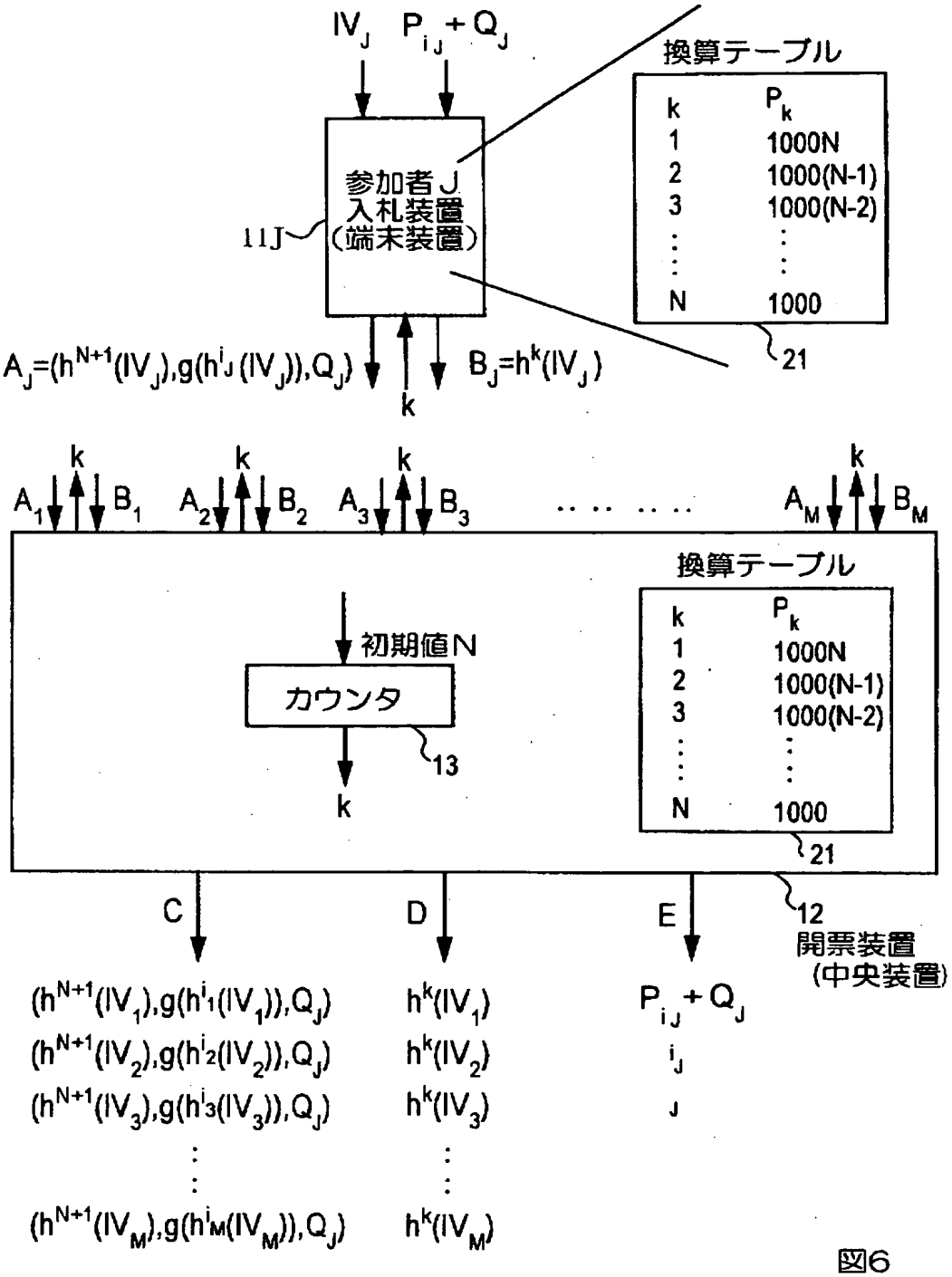
IV_J
P_iJ + Q_J
換算テーブル
k
P_k
1
1000N
2
1000(N-1)
3
1000(N-2)
N
1000
21
参加者Ｊ
入札装置
(端末装置)
11J
A_J=(h^{N+1}(IV_J),g(h^{iJ}(IV_J)),Q_J)
B_J=h^k(IV_J)
k
A_1 B_1 A_2 B_2 A_3 B_3 A_M B_M
初期値Ｎ
カウンタ
13
C
D
E
12
開票装置
(中央装置)
(h^{N+1}(IV_1),g(h^{i1}(IV_1)),Q_J)
(h^{N+1}(IV_2),g(h^{i2}(IV_2)),Q_J)
(h^{N+1}(IV_3),g(h^{i3}(IV_3)),Q_J)
(h^{N+1}(IV_M),g(h^{iM}(IV_M)),Q_J)
h^k(IV_1)
h^k(IV_2)
h^k(IV_3)
h^k(IV_M)
P_iJ + Q_J
iJ
J

図6

【図７】

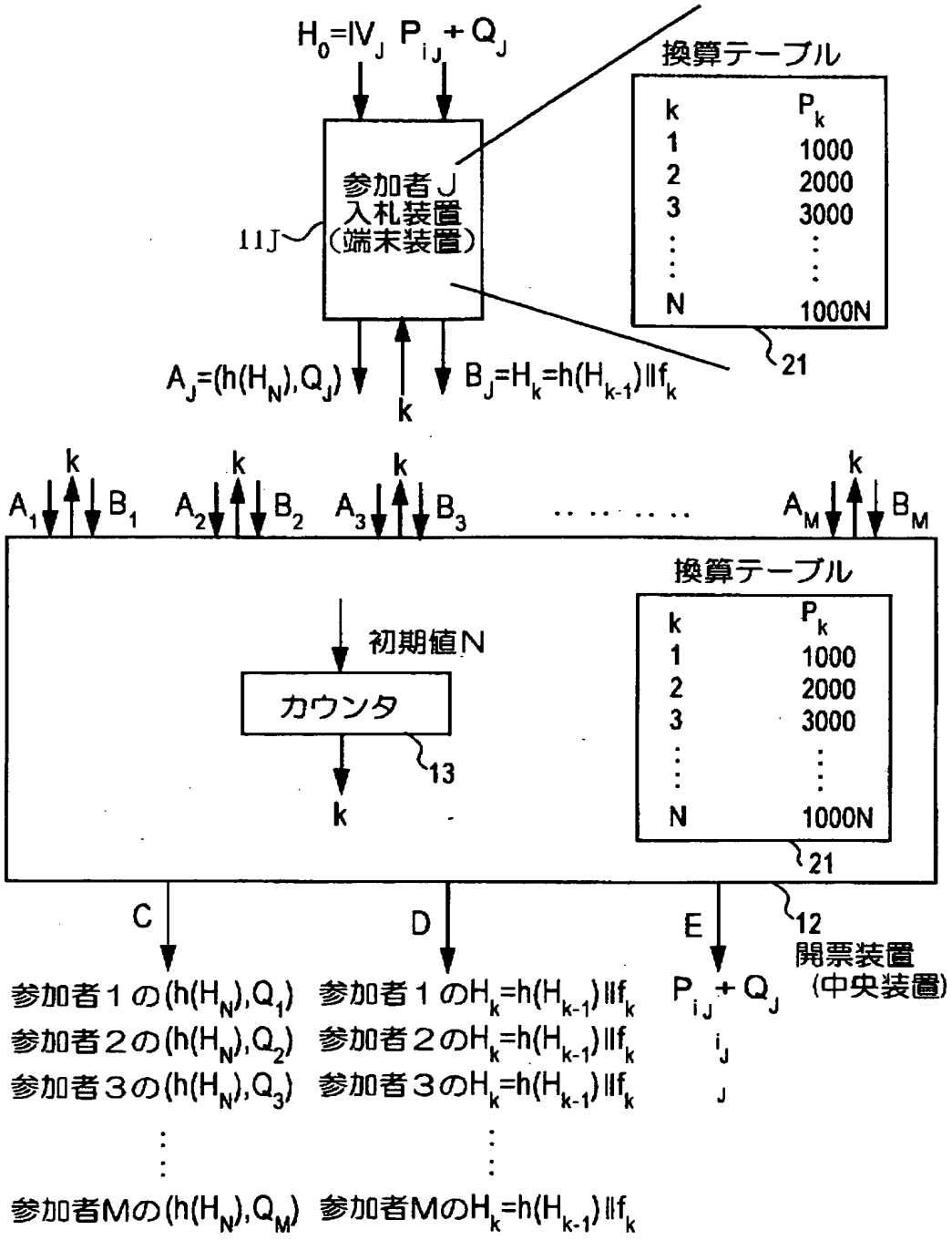
$H_0=IV_J\ P_{iJ}+Q_J$
換算テーブル
k
P_k
1
1000
2
2000
3
3000
N
1000N
21
参加者Ｊ
入札装置
(端末装置)
11J
$A_J=(h(H_N),Q_J)$
$B_J=H_k=h(H_{k-1})\|f_k$
k
A_1 B_1 A_2 B_2 A_3 B_3 A_M B_M
初期値N
カウンタ
13
C
D
E
12
開票装置
(中央装置)
参加者１の$(h(H_N),Q_1)$
参加者２の$(h(H_N),Q_2)$
参加者３の$(h(H_N),Q_3)$
参加者Mの$(h(H_N),Q_M)$
参加者１の$H_k=h(H_{k-1})\|f_k$
参加者２の$H_k=h(H_{k-1})\|f_k$
参加者３の$H_k=h(H_{k-1})\|f_k$
参加者Mの$H_k=h(H_{k-1})\|f_k$
$P_{iJ}+Q_J$

図7

【図８】

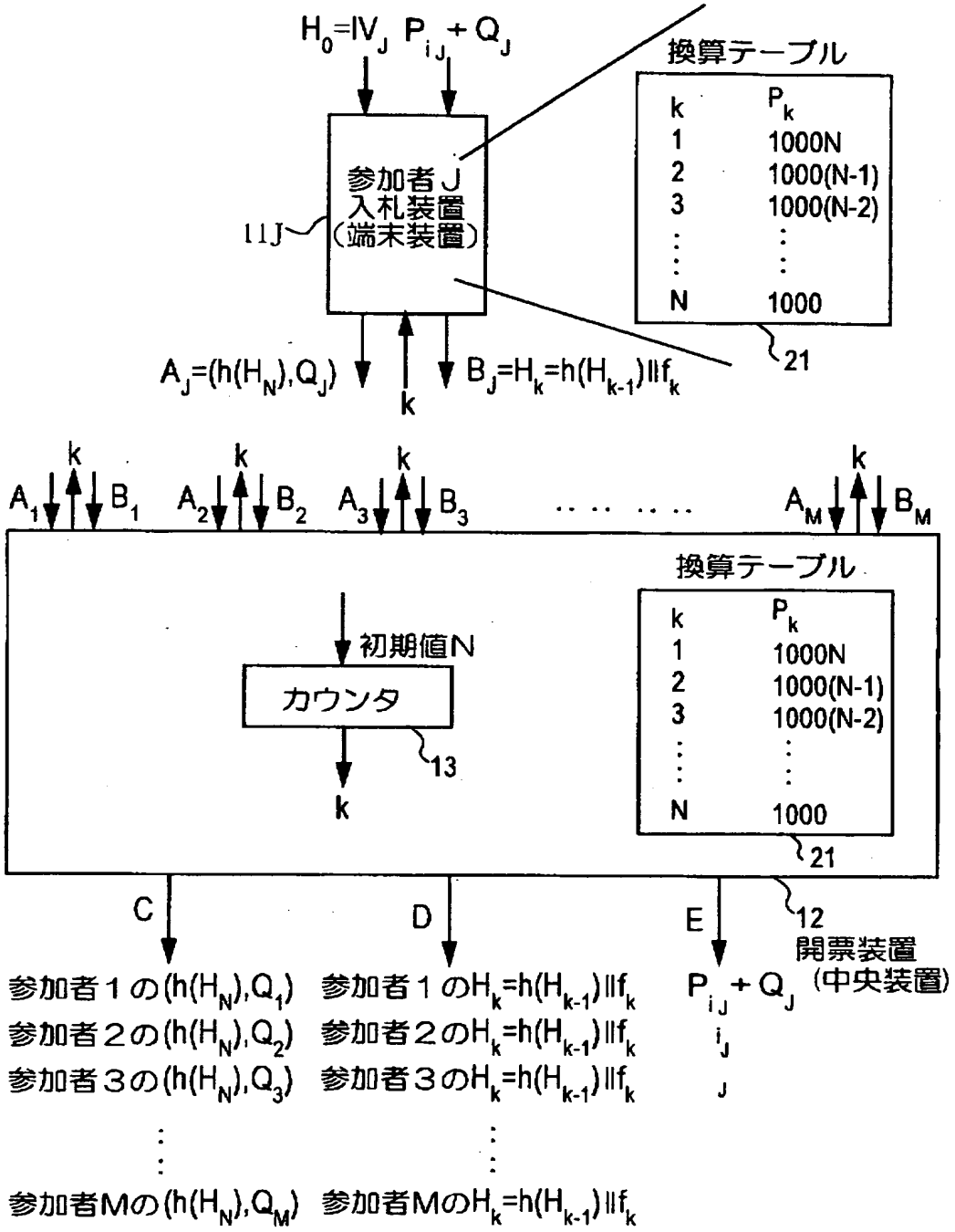
$H_0=IV_J\ P_{i_J}+Q_J$
換算テーブル
k　P_k
1　1000N
2　1000(N-1)
3　1000(N-2)
N　1000
21
参加者Ｊ
入札装置
(端末装置)
11J
$A_J=(h(H_N),Q_J)$
k
$B_J=H_k=h(H_{k-1})\|f_k$
A_1 B_1 A_2 B_2 A_3 B_3 ．．．．．． A_M B_M
初期値N
カウンタ
13
C
D
E
12
開票装置
(中央装置)
参加者１の$(h(H_N),Q_1)$
参加者２の$(h(H_N),Q_2)$
参加者３の$(h(H_N),Q_3)$
参加者Mの$(h(H_N),Q_M)$
参加者１の$H_k=h(H_{k-1})\|f_k$
参加者２の$H_k=h(H_{k-1})\|f_k$
参加者３の$H_k=h(H_{k-1})\|f_k$
参加者Mの$H_k=h(H_{k-1})\|f_k$
$P_{i_J}+Q_J$
i_J
J

図8

【図９】

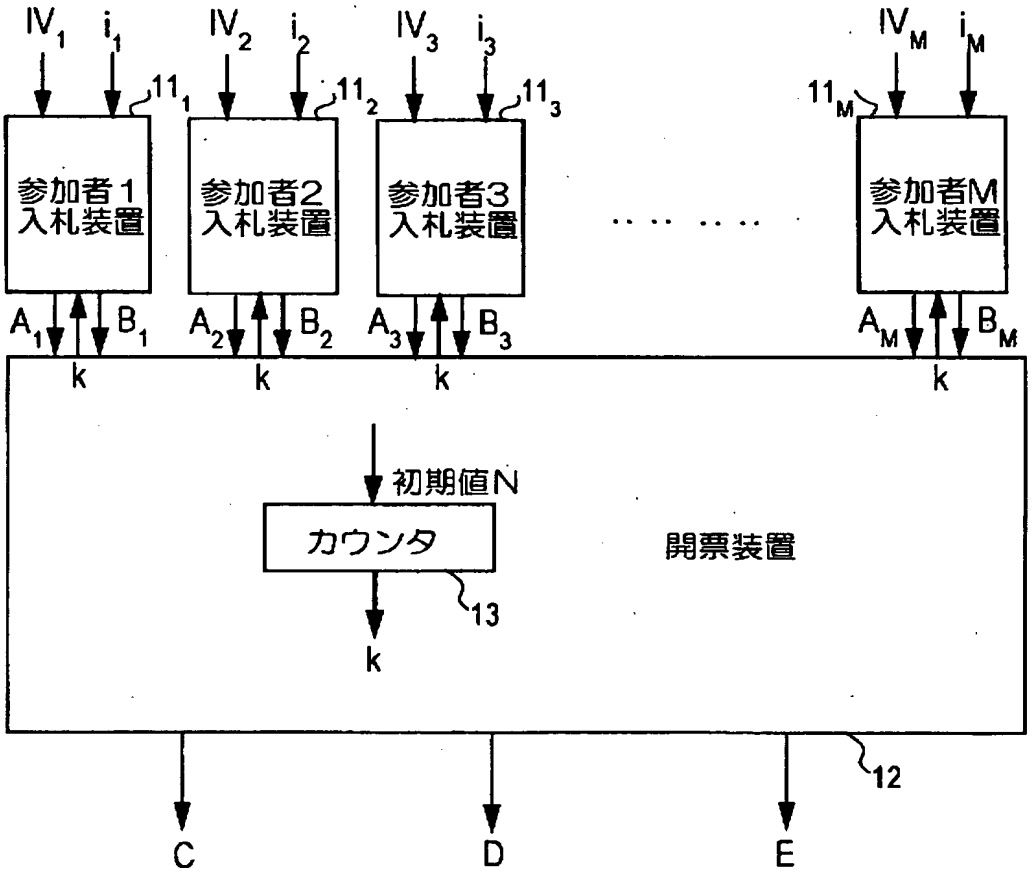
IV1
i1
IV2
i2
IV3
i3
IVM
iM
11
11
11
11
M
参加者１
入札装置
参加者2
入札装置
参加者3
入札装置
参加者M
入札装置
A1
B1
A2
B2
A3
B3
AM
BM
k
k
k
k
初期値N
カウンタ
開票装置
13
k
12
C
D
E

図9

【書類名】　　要約書

【要約】

【課題】　例えば電子競争入札において同一構成、同一処理で最大値又は最小値を求めることを可能とする。

【解決手段】　指標値（ｋ）１，２，…，Ｎと対応する値（P_k）P_1，P_2，…，P_Nとの換算テーブル２１を入札装置、開票装置１２に設け、参加者Ｊは入札値P_{iJ}と対応した指標値i_Jを求め、Ｊの初期値IV_Jを初期として多重ハッシュした値$h^{N+1}(IV_J)$と$g(h^i_J(IV_J))$を求め、開票装置１２へ送り、全参加者が登録し終ると、装置１２はＮから順に登録したかの問合せを全参加者へ送り、指標値ｍに対して、各参加者は$h^m(IV_J)$を返送し、登録してある$g(h^i_J(IV_J))$と一致したものを受信すると、その時のｍを登録中の最高指標値とし、その登録した値を明らかにする、テーブル２１が指標１，…，Ｎに対し$P_1<\cdots<P_N$であれば入札最大値が求まり、テーブル２１が１，…，Ｎに対し$P_1>\cdots>P_N$であれば入札最小値が求まる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　　住所変更
住　所　　東京都千代田区大手町二丁目３番１号
氏　名　　日本電信電話株式会社